

### REMARKS

Applicant appreciates the detailed examination evidenced by the Office Action mailed October 27, 2008 (hereinafter "Office Action"). Applicant has amended Claims 4, 9, 12, 13 and 22 as set out above and respectfully submits that these claims are in compliance with Section 112. Applicant respectfully submits that the pending claims are in condition for allowance for at least the reasons discussed herein.

#### **The Section 112 Rejections**

Claims 4, 9, 12, 13 and 22 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. *See* Office Action, page 3. Applicant will address each of the rejections below.

With respect to Claims 4 and 12, the Office Action objects to the phrase "the pre-defined area" as having insufficient antecedent basis. *See* Office Action, page 3. Claims 4 and 12 recite "wherein an area of the security data in the non-volatile memory and an area for storage of the security data in the working memory are pre-defined." Thus, Claims 4 and 12 recite two pre-defined areas, a pre-defined area for the security data in the non-volatile memory and a pre-defined area for storage of the security data in the working memory. Accordingly, Applicant has amended Claims 4 and 12 to recite "the pre-defined area for storage of the security data in the working memory" to further clarify the pre-defined area being referred to in Claims 4 and 12. Accordingly, Applicant respectfully requests that the Section 112 rejection with respect to Claims 4 and 12 be withdrawn for at least these reasons.

With respect to Claim 9, the Office Action objects to the phrase "the data processing environment" as having insufficient antecedent basis. *See* Office Action, page 3. Applicant has amended Claim 9 as set out above and, therefore, respectfully requests withdrawal of the Section 112 rejections with respect to Claim 9 for at least these reasons.

With respect to Claims 13 and 22, the Office Action objects to the phrase "the pre-defined area" as having insufficient antecedent basis. *See* Office Action, page 3. Claims 13 and 22 recite "wherein an area of the security data in the non-volatile memory is pre-defined and pre-stored in the device." Thus, Claims 13 and 22 recite a pre-defined area of the security data in the non-volatile memory that is pre-stored in the device. Accordingly,

Applicant has amended Claims 13 and 22 to recite "the pre-defined area of the security data in the non-volatile memory" to further clarify the pre-defined area being referred to in Claims 13 and 22. Accordingly, Applicant respectfully requests that the Section 112 rejection with respect to Claims 13 and 22 be withdrawn for at least these reasons.

### **The Section 102 Rejections**

Claims 1-6, 8-13, 15, 16, 18-22 and 24-27 stand rejected under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 6,115,819 to Anderson (hereinafter "Anderson"). *See* Office Action, page 4. Applicant respectfully submits that many of the recitations of these claims are neither disclosed nor suggested by Anderson for at least the reasons discussed herein. For example, independent Claim 1 recites:

A method of transferring data from a non-volatile memory to a working memory of an electronic data processing device, comprising:

**copying security data from the non-volatile memory to the working memory, wherein the security data is to be write-protected;**

**activating a blocking function for the security data in the working memory, wherein activating is triggered by the copying being made to the working memory;**

monitoring all communication with the working memory; and

blocking all write attempts to the copied security data stored in the working memory according to the blocking function, wherein at least activating a blocking function, monitoring communication and blocking write attempts are performed independently of a central processing unit of the electronic data processing device, such that the central processing unit cannot manipulate the security data.

Independent Claim 9 contains corresponding device recitations. Applicant respectfully submits that at least the highlighted recitations of independent Claim 1 are neither disclosed nor suggested by Anderson for at least the reasons discussed herein.

The Office Action points to Figure 1 and related portions of Anderson as teaching all of the recitations of Claim 1. *See* Office Action, pages 4-5. Anderson discusses an access monitor that is configured to monitor "every data transfer that occurs on the system bus." *See* Anderson, column 4, lines 34 – 40. Furthermore, the access monitor discussed in Anderson is also configured to disable transactions to a memory via a security gate. *See* Anderson, column 4, lines 59 – 65. The disabled transactions mentioned relate to "access to a memory location" during current the current instruction. *See* Anderson, column 6, line 49 – 50. Anderson also discusses write operations at column 6, lines 38 – 40. Accordingly, Anderson

discusses a system including an access monitor that is configured to allow or disable access to different memories. Thus, Anderson discusses a static scenario, where security measures are in place from the beginning. Nothing in Anderson discloses or suggests at least the highlighted portion of Claim 1 set out above.

In particular, the Office Action points to the following portion of Anderson as teaching “copying security data from the non-volatile memory to the working memory, wherein the security data is to be write-protected” as recited in Claim 1 (*See* Office Action, page 4):

Restrictions on the exchange or transfer of data between various elements of the system is controlled by the AM 28 which has control of gates 32-48 which are physically located between the system bus and various I/o devices and system memory.

Anderson, column 6, lines 15-19. The cited portion of Anderson generically discusses the exchange or transfer of data. Nothing in the cited portion of Anderson discusses copying security data from the non-volatile memory to the working memory wherein the security data is to be write-protected as recited in Claim 1. Since anticipation requires that each and every recitation of the claims be taught by the cited reference, Applicant respectfully submits that independent Claim 1 and the claims that depend therefrom are patentable over Anderson for at least these reasons.

Furthermore, the Office Action points to the following portion of Anderson as teaching “activating a blocking function for the security data in the working memory, wherein activating is triggered by the copying being made to the working memory” as recited in Claim 1 (*See* Office Action, page 4):

In one example the access monitor is adapted to control the central processing unit and may in a preferred made of operation reset the central processing unit upon being initiation or being installed in the computer system, or at the time of other predetermined events.

Anderson, column 4, lines 46-50. The cited portion of Anderson generally discusses the access monitor, but nothing in the cited portion of Anderson discusses activating a blocking function for the security data in the working memory, wherein activating is *triggered by the copying being made to the working memory* as recited in Claim 1. Since anticipation requires that each and every recitation of the claims be taught by the cited reference,

Applicant respectfully submits that independent Claim 1 and the claims that depend therefrom are patentable over Anderson for at least these reasons.

As discussed above, independent Claim 9 contains corresponding device recitations to the recitations of Claim 1. The Office Action rejects Claim 9 based on the same portions of Anderson discussed above with respect to Claim 1. *See* Office Action, page 7. Accordingly, Applicant respectfully submits that independent Claim 9 and the claims that depend therefrom are patentable over Anderson for at least the reasons discussed above with respect to Claim 1.

As discussed above the dependent claims are patentable over Anderson at least per the patentability of the independent base claims from which they depend. However, many of the dependent claims are also separately patentable for at least the reasons discussed herein.

For example, Claim 3 recites, in part:

wherein copying data comprises copying **only the security data from the non-volatile memory to the working memory** independently of the central processing unit of the data processing device and copying any further data under the control of the central processing unit of the device.

Dependent Claims 11 and 19 contain corresponding device recitations. The Office Action points to column 6, lines 26-31 of Anderson as teaching all of the recitations of Claim 3. *See* Office Action, page 5. The cited portion of Anderson discusses the CPU and circumstances where the CPU requires access to a particular memory location. Nothing in the cited portion of Anderson discloses or suggests copying only the security data from the non-volatile memory to the working memory as recited in Claim 3. Accordingly, Applicant respectfully submits that dependent Claims 3, 11 and 19 are separately patentable over Anderson for at least these reasons.

The Office Action cites the same portion of Anderson as teaching all the recitations of dependent Claims 4, 12 and 20. *See* Office Action, pages 6, 9 and 10. As discussed above, the cited portion of Anderson discusses the CPU and circumstances where the CPU requires access to a particular memory location. Nothing in the cited portion of Anderson discloses or suggests the details of pre-defined areas and activating a blocking function as recited in Claims 4, 12 and 20. Accordingly, Applicant respectfully submits that dependent Claims 4, 12 and 20 are separately patentable over Anderson for at least these reasons.

By way of final example, dependent Claim 8 recites:

The method of Claim 1, further comprising disconnecting a debugging unit at least when copying the security data to the working memory and reconnecting the debugging unit when the blocking function has been activated.

Dependent Claims 15 and 24 contain similar recitations. The Office Action points to the following portions of Anderson as teaching all of the recitations of Claim 8 (*See* Office Action, page 7):

By monitoring the signals on the system bus the access monitor can determine the details of every data access that takes place, ie the address of the data being accessed and whether the access is a read or a write access. **If the access monitor decides that the transaction is not permitted then it can disable the gate through which the data transfer would occur.** When the CPU (central processing unit) of the system tries to perform a data transfer through a disabled gate, a memory access fault is generated.

Anderson, column 4, lines 59-67 (emphasis added). The cited portion of Anderson discusses disabling the gate, not the debugging unit as recited in Claim 8. According, Applicant respectfully submits that dependent Claims 4, 15 and 24 are separately patentable over Anderson for at least these additional reasons.

### **The Section 103 Rejections**

A. Claims 7 and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Anderson in view of United States Patent Publication No. 2003/0226029 to Porter (hereinafter "Porter"). *See* Office Action, page 12. Applicant respectfully submits that the dependent claims are patentable at least per the patentability of the independent base claims from which they depend.

B. Claim 17 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 4,489,380 to Carey (hereinafter "Carey") in view of Anderson. *See* Office Action, page 14. Applicant respectfully submits that many of the recitations of Claim 17 are neither disclosed nor suggested by the cited combination. For example, independent Claim 17 recites:

An electronic data processing device comprising:  
a non-volatile memory comprising data including security data to be write-protected;  
a working memory;

a central processing unit configured to control copying of at least some data from the non-volatile memory to the working memory; and

a device for blocking write attempts to security data transferred from the non-volatile memory to the working memory and comprising a monitoring unit configured to:

**activate a blocking function for security data in the working memory, which activation is triggered by a copying of the security data being made from the non-volatile memory to the working memory;**

monitor all communication with the working memory; and

block all write attempts to the copied security data stored in the working memory according to the blocking function, all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data.

As discussed above with respect to Claim 1, at least the highlighted recitations of Claim 17 are neither disclosed nor suggested by Anderson. Furthermore, nothing in Carey provides the missing teachings. Accordingly, Applicant submits that independent Claim 17 and the claims that depend therefrom are patentable over the cited combination for at least the reasons discussed herein.

Furthermore, Applicant respectfully submits that there is no motivation to combine the cited references as suggested in the Office Action. As discussed above, Anderson discusses an environment, where there is a static safety measure provided. Anderson discusses a static scenario where data is protected by an access monitor and security gate and that does not react to change. This is further supported by column 5, lines 4-9 of Anderson, where it is mentioned that in order to change the access policy, the access monitor must be replaced by another access monitor with the changed security policy. In other words, it is not possible to change settings when copying is being made.

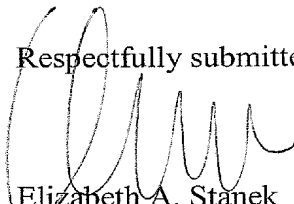
In stark contrast, embodiments of the present invention are directed towards solving the problem of transferring security data from a non-volatile memory to a working memory in a safe way as recited in, for example, Claim 17. Embodiments of the present invention provide write protection of a working memory when the security data has been copied. Before that it is possible to use the area for other purposes. Accordingly, one of skill in the art would not be motivated to modify Anderson, a static scenario, with any of the other cited references to provide the recitations of the claims of the present application, as such a change would render the teachings of Anderson useless. Applicant respectfully submits that the pending claims are patentable over the cited combination for at least these additional reasons.

C. Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Carey in view of Anderson in further view of Porter. *See* Office Action, page 17. Applicant respectfully submits that the dependent claims are patentable at least per the patentability of the independent base claims from which they depend.

### CONCLUSION

As all of the claims are now in condition for allowance, Applicant respectfully requests allowance of the claims and passing of the application to issue in due course. Applicant urges the Examiner to contact Applicant's undersigned representative at (919) 854-1400 to resolve any remaining formal issues.

Respectfully submitted,

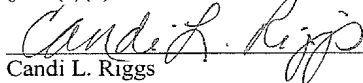


Elizabeth A. Stanek  
Registration No. 48,568  
Attorney for Applicant

**USPTO Customer No. 54414**  
Myers Bigel Sibley & Sajovec  
Post Office Box 37428  
Raleigh, North Carolina 27627  
Telephone: 919/854-1400  
Facsimile: 919/854-1401

### CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on January 27, 2009.

  
Candi L. Riggs